BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 40 15 482 C 1**

(51) Int. Cl.[5]:
G 06 F 12/14
G 07 C 9/00

(21) Aktenzeichen: P 40 15 482.3-53
(22) Anmeldetag: 14. 5. 90
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 25. 7. 91

DE 40 15 482 C1

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:

Competence Center Informatik GmbH, 4470 Meppen, DE

(74) Vertreter:

Pagenberg, J., Dr.jur.; Frohwitter, B., Dipl.-Ing., Rechtsanwälte; Geißler, B., Dipl.-Phys.Dr.jur., Pat.- u. Rechtsanw.; Bardehle, H., Dipl.-Ing.; Dost, W., Dipl.-Chem. Dr.rer.nat.; Altenburg, U., Dipl.-Phys., Pat.-Anwälte, 8000 München

(72) Erfinder:

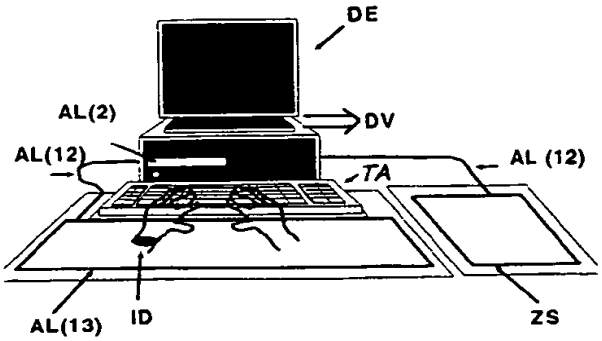
Holzapfel, Stephan, 4470 Meppen, DE; Book, Nobert, 4530 Ibbenbüren, DE; Kraaibeek, Peter, 4450 Lingen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US-Z, IBM Technical Disclosure Bulletin, Vol. 31, No. 9, Februar 1989, S. 223;
DE-Z, Funkschau 13/1986, S. 24-28, Firmenschrift der Unina, Unises, a revolutionary 100% watertightsecurrty system for your PC;

(54) System zur berührungslosen Authentisierung des Nutzers einer Datenendeinrichtung eines Datenverarbeitungssystems

(57) Es wird ein System zur berührungslosen Authentisierung des Nutzers einer Datenendeinrichtung eines Datenverarbeitungssystems angegeben. Der Nutzer trägt, schwer verlierbar, einen Identifikationsträger mit sich, der innerhalb einer Entfernung von weniger als 1 m abgefragt werden kann. Ein Abstandsleser, der nahe bei der Datenendeinrichtung angebracht und über ein Verbindungskabel mit ihr verbunden ist, fragt kontinuierlich die persönliche Nutzerkennung auf dem Identifikationsträger ab. Wenn die vorbestimmte Entfernung für vorbestimmte Zeitspannen überschritten wird, so wird die Datenendeinrichtung teilweise oder ganz blockiert. Ein Schreibgerät programmiert den Identifikationsträger zu vorgegebenen Zeitpunkten, an denen der Nutzer anderweitig identifiziert wird. Das Schreibgerät übermittelt die erzeugte Nutzerkennung an das Datenverarbeitungssystem. Sowohl bei der Abfrage als auch bei der Programmierung der persönlichen Nutzerkennung befindet sich der Identifikationsträger in einem magnetischen Wechselfeld.



DE 40 15 482 C1

Beschreibung

Die Erfindung bezieht sich auf ein System zur Authentisierung des Nutzers einer Dateneinrichtung eines Datenverarbeitungssystems, wie es im Oberbegriff des Patentanspruchs 1 angegeben ist. Ein derartiges System ist aus einer Firmenschrift der Firma UNINA bekannt, in welcher das Sicherheitssystem UNISES beschrieben ist. Die Erfindung bezieht sich ferner auf ein System zur Authentisierung nach dem Oberbegriff des Patentanspruchs 13.

Um gefährdete oder anderweitig schutzwürdige Datenverarbeitungssysteme vor unberechtigtem Zugriff zu schützen, werden üblicherweise sogenannte LOGON-Verfahren eingesetzt. Hierzu werden an einer Datenendeinrichtung des Datenverarbeitungssystems Nutzerkennungen und Paßwörter eingegeben, die dem autorisierten Nutzer und dem System bekannt sind. Das System identifiziert den Nutzer anhand seines Paßworts und gewährt ihm an der benutzten Datenendeinrichtung die zugewiesenen Zugriffsrechte.

Dieses Verfahren weist Schwächen auf, durch welche ein Paßwort verhältnismäßig leicht umgangen werden kann:

- Simple Paßworte sind leicht aufdeckbar; der Schutz des Systems vor unberechtigten Nutzern ist nicht gewährleistet.
- Wirksame und damit lange Paßworte werden vom autorisierten Nutzer leicht vergessen. Daher werden diese häufig schriftlich aufgezeichnet und können ebenfalls aufgedeckt werden.
- Nutzern, die ihr Identifikationsmerkmal "Paßwort" vergessen haben, stehen die Systemleistungen in kritischen Situationen nicht zur Verfügung.
- Der Vorgang des LOGON belastet den Nutzer zeitlich und lenkt ihn von der eigentlichen Nutzung des Systems ab.
- Paßworte können bei der Eingabe über die Tastatur durch Beobachten der Finger ausgespäht werden.

Die aufgeführten Unzulänglichkeiten machen die autorisierte Nutzung des Datenverarbeitungssystems unbequem. Hieraus resultiert häufig die eingeschränkte oder unzulängliche Nutzung der verfügbaren Sicherheitsmechanismen.

Die vorhandenen Sicherheitsmängel haben zu Überlegungen geführt, wie die Datensicherheit bei Benutzung einer Dateneinrichtung grundsätzlich verbessert werden könnte. Das eingangs erwähnte Sicherheitssystem UNISES verzichtet auf die manuelle Eingabe von Paßwörtern und authentisiert den Nutzer eines Personal-Computers automatisch. Die Vorrichtung besteht aus einem integrierten Schaltkreis, der im Personal-Computer eingebaut und mit leistungsfähigen Verschlüsselungsfunktionen versehen ist, sowie aus einem kleinen Hochfrequenzsender, der in einer Tasche des Nutzers getragen wird und eine persönliche Kennung aktiv abstrahlt. Der Hochfrequenzsender hat eine Reichweite von 5 Metern und die Funkverbindung selbst ist bereits durch Verschlüsselungsalgorithmen geschützt. Wenn der Personal-Computer einen berechtigten Nutzer identifiziert, dann wird die Kennung aus dem Identifikationsträger in den Verschlüsselungs-Chip übertragen und es stehen außer den Standardfunktionen des Personal-Computers auch die geschützten Datenbereiche zur Verfügung. Die Authentisierung wird kontinuierlich wiederholt. Wenn der Benutzer seinen Arbeitsplatz verläßt, dann führt der Personal-Computer die normale Datenverarbeitung fort; jedoch sperrt er jeden Zugang zu den Eingabegeräten (beispielsweise zu der Tastatur).

Dieses Autorisierungsverfahren erfüllt bereits einige der Bedingungen, die an einen verbesserten Datenschutz zu stellen sind. Insbesondere wird die Unterscheidung zwischen autorisierten und nicht-autorisierten Personen möglich, ohne daß der zugangsberechtigte Nutzer umständliche und zeitraubende Eingabeprozeduren vornehmen muß. Wenn sich der autorisierte Nutzer entfernt, wird der Personal-Computer automatisch in seinen sicherheitsempfindlichen Funktionen blokkiert. Nachteilig an dem bekannten Verfahren ist der aktive, d. h. batteriebetriebene und daher nicht wartungsfreie, sowie vergleichsweise voluminöse Sender. Nachteilig ist ferner, daß das unbekannte Verfahren nicht offen ist für weitere Authentisierungsschritte, die um so wichtiger werden, je größer das Datenverarbeitungssystem ist, an welches die Datenendeinrichtung angeschlossen ist.

Aus dem IBM Technical Disclosure Bulletin, Februar 1989, S. 223 und aus Funkschau 13/1986, S. 24—29 sind kleine, passive Identifikationsträger bekannt.

Die Erfindung hat sich die Aufgabe gestellt, bei einem berührungslosen Autentisierungsverfahren der vorausgesetzten Art den Schutz der persönlichen Nutzerkennung gegen Verlust oder Ausspähung weiter zu verbessern. Diese Aufgabe wird durch die kennzeichnenden Merkmale des Anspruchs 1 in Verbindung mit den Gattungsmerkmalen gelöst. Eine nebengeordnete Ausprägung des Erfindungsgedankens ist im Anspruch 13 angegeben.

Der erfindungsgemäße Identifikationsträger ist passiv, wartungsfrei und nicht größer als $3 \times 15 \times 20$ mm. Bei dem erfindungsgemäßen System kann die Nutzerkennung auf dem Identifikationsträger häufig, zum Beispiel täglich, gewechselt werden. Hierzu werden die Nutzerkennungen von einer Stelle ausgegeben, die den Nutzer täglich auf Grund anderer Merkmale eindeutig identifiziert. Die neue Nutzerkennung wird dabei von einem an der ausgebenden Stelle installierten Schreibgerät erzeugt und in Verbindung mit der persönlichen Autentisierung durch die ausgebende Stelle automatisch an das System übermittelt. Das Schreibgerät kann mit einem der Abstandsleser kombiniert sein, der die Kennung aus dem Identifikationsträger ausliest und an die Datenendeinrichtung weitergibt.

Für die tägliche Autentisierung des Nutzers bei Übernahme der Kennung können biometrische Identifikationsverfahren zum Einsatz kommen, die zu kostenträchtig wären, wenn sie für jede Datenendeinrichtung eingesetzt würden. Beispielsweise kann die biometrische Identifikation eine automatische Auswertung der Unterschrift sein. In einem typischen Anwendungsbeispiel betritt ein Datenverarbeitungsnutzer das Betriebsgebäude seiner Firma und weist sich am Eingang durch Unterschrift aus. Statt einer automatischen Auswertung der Unterschrift kommt auch eine persönliche Identifizierung in Betracht. Er erhält daraufhin einen Identifikationsträger oder, falls er einen solchen schon besitzt, eine neue Kennung zur Nutzung des hausinternen Datenverarbeitungssystems. Die Kennung wird von einem Schreibgerät einprogrammiert und zusammen mit der Identität des Nutzers an das Datenverarbeitungssystem gemeldet. Das System gibt die Tageskennung dieses Nutzers gegebenenfalls an zusätzlich zu nutzende Sub-

systeme weiter.

Die Identifikationsträger ist mit dem Nutzer schwer verlierbar in der Nähe des Handgelenks verbunden. Beispielsweise kann der Identifikationsträger an einem Armband festgeklammert werden; er kann aber auch in eine Uhr, einen Armreif oder sogar einen Fingerring fest eingelassen sein. Nach der Übernahme des Identifikationsträgers oder der neuen Kennung begibt sich der Nutzer an seinen Arbeitsplatz. Die Datenendeinrichtung erkennt den Nutzer anhand der Kennung im Identifikationsträger. Hierzu ist in der Datenendeinrichtung ein Abstandsleser eingebaut, der jeden Nutzer in der Nähe der Datenendeinrichtung eindeutig identifiziert. Der Abstandsleser wird von einem speziellen Programm gesteuert, welches für den identifizierten Nutzer sofort und automatisch den LOGON-Vorgang über die Datenendeinrichtung auslöst. Der Nutzer kann ohne Verzögerung mit seiner Tätigkeit im Datenverarbeitungssystem beginnen. Der LOGON-Vorgang kann in den Fällen, in denen ein vollautomatischer Ablauf nicht sinnvoll ist, zusätzlich vom Nutzer aktiv angestoßen werden. Der Ablauf des LOGON wird an der Datenendeinrichtung angezeigt.

Bei der Kommunikation zwischen Datenendeinrichtung und Rechner können während des LOGON kryptographische Verfahren zum Einsatz kommen, die ein Aufdecken der Nutzerkennung durch Abhören von Leitungen erschweren.

Die Authentisierung des an der Datenendeinrichtung tätigen Nutzers wird periodisch oder kontinuierlich wiederholt. Im Verlauf des Tages verläßt der Nutzer häufig für verschieden lange Zeitspannen seinen Arbeitsplatz. Die Authentisierungsvorrichtung erkennt dies und sperrt sofort für die Zeit der Abwesenheit die Eingabe und/oder Ausgabe der Datenendeinrichtung bei längeren Abwesenheiten wird ein LOGOFF durchgeführt. Zu diesem Zweck wird die Authentisierung des an der Datenendeinrichtung tätigen Nutzers periodisch oder kontinuierlich wiederholt. Verläßt der Nutzer den Wirkungsbereich des Abstandslesers, der maximal einen Meter beträgt, so wird von dem Ansteuerungsprogramm des Abstandslesers beispielsweise die Tastatur gesperrt oder der Bildschirm dunkel getastet. Die Blokkierung erfolgt so lange, bis der Nutzer wieder in den Wirkungsbereich des Abstandslesers zurückkehrt oder durch eine Zeitschaltung des Ansteuerungsprogramms das Abmelden des Nutzers beim System ausgelöst wird.

Die verschiedenen Sperrfunktionen der Datenendeinrichtung können ebenfalls ausgelöst werden, wenn ein nicht autorisierter Nutzer in den Wirkungsbereich des Abstandslesers kommt. Hierzu sind gegebenenfalls weitere Sensoren einzusetzen, die hier nicht beschrieben werden.

Wechseln im Tagesverlauf die Nutzer an einer Datenendeinrichtung, so wird für den jeweils berechtigten Nutzer sofort ein neues LOGON durchgeführt. Jedoch kann der ehemalige Nutzer durch Auslösen einer Sperrfunktion des Abstandslesers diesen Vorgang unterbinden, beispielsweise um einem Mitarbeiter einen Eingabe- oder Ausgabevorgang unmittelbar an der Datenendeinrichtung zu zeigen.

Am Ende des Arbeitstages gibt der Nutzer seinen Identifikationsträger oder seine Kennung an die zentrale Ausgabestelle zurück, wobei seine Kennung abgefragt und dem Datenverarbeitungssystem die Ungültigkeit dieser Kennung mitgeteilt wird.

Der Abstandsleser besteht prinzipiell aus einer Sende- und Empfangsspule sowie einer elektronischen Baugruppe. Typischerweise ist zumindest die Sende- und Empfangsspule sehr nahe bei der Eingabetastatur angebracht. Im Betrieb umgibt sie sich mit einem niederfrequenten magnetischen Wechselfeld, dessen Reichweite typischerweise bei 5—20 cm liegt. Das magnetische Wechselfeld reagiert auf die Anwesenheit des Identifikationsträgers, der am Handgelenk des beispielsweise vor dem Bildschirm sitzenden und die Tastatur berührenden Nutzers angebracht ist.

Die Erfindung wird anhand der Zeichnungsblätter mit den Fig. 1—6 näher beschrieben. Es zeigt

Fig. 1: Die Hauptkomponenten des erfindungsgemäßen Authentisierungssystems

Fig. 2: ein Blockschaltbild des Identifikationsträgers, während er sich im magnetischen Wechselfeld des Schreibgeräts befindet

Fig. 3: drei verschiedene Bauformen des Identifikationsträgers

Fig. 4: ein Blockschaltbild des Abstandslesers

Fig. 5: eine mögliche Bauform des Abstandslesers

Fig. 6: ein Flußdiagramm des im Abstandsleser benutzten Abfrageprogramms.

In Fig. 1 ist mit DE eine Datenendeinrichtung bezeichnet, die mit einem Datenverarbeitungssystem DV, typischerweise einem zentral aufgestellten Rechner verbunden ist. Als Datenendeinrichtung ist in diesem Ausführungsbeispiel ein Personal-Computer vorgesehen; es kann sich jedoch auch um eine sogenannte Arbeitsstation (work station) oder um ein einfaches Terminal handeln. Im gezeichneten Ausführungsbeispiel steht auf der Zentraleinheit des Personal-Computers ein Bildschirm, während vor der Zentraleinheit in üblicher Weise eine Tastatur TA liegt. Nahe bei der Datenendeinrichtung DE und elektrisch mit ihr verbunden, ist ein Abstandsleser AL angeordnet. Im gezeichneten Ausführungsbeispiel ist ein Abstandsleser AL angeordnet. Im gezeichneten Ausführungsbeispiel ist die Sende- und Empfangsspule 13 des Abstandslesers AL in die Schreibtischunterlage vor der Tastatur TA eingewirkt. Die Sende- und Empfangsspule 13 ist über eine Verbindungsleitung 12 an eine elektronische Baugruppe 2 des Abstandslesers AL angeschlossen, welche als spezifische Prozessor-Karte einschließlich des zugehörigen Sicherheitsprogramms einen Steckplatz des Personal-Computers belegt. Die elektronische Baugruppe 2 kann jedoch auch zusammen mit der Sende- und Empfangsspule 13 in einen Vorlegekeil eingebaut sein, der sich gleichfalls in der Nähe der Tastatur TA befindet. In diesem Fall ist der Abstandsleser AL über eine externe Schnittstelle mit dem Personal-Computer verbunden.

Mit dem Bezugszeichen ID ist ein Identifikationsträger angedeutet, der sich zwangsläufig in der Reichweite des magnetischen Wechselfelds des Abstandslesers AL aufhält, wenn ein Nutzer der Datenendeinrichtung DE ihn am Handgelenk oder in der Nähe des Handgelenks befestigt hat. Mit ZS ist ein zum Abstandsleser AL alternativer Zusatzsensor angedeutet, der es als Option ermöglicht, eine Maussteuerung in die geschützten Eingabefunktionen einzubeziehen.

Der Identifikationsträger ID wird vom Nutzer zum Beispiel in Form einer Uhr oder eines Armbandes getragen. Die Benutzeridentifikation für das LOGON erfolgt im gezeichneten Ausführungsbeispiel, sobald sich der Identifikationsträger ID unmittelbar über der Sende- und Empfangsspule 13 des Abstandslesers AL befindet. Die maximale Abfrageentfernung ist typischerweise kleiner als 20 cm. Die vorbestimmte Entfernung, in welcher die Abfrage der Kennung noch möglich ist, beträgt

in jedem Fall weniger als 1 Meter.

Der Identifikationsträger ID besteht im wesentlichen aus 2 Komponenten. Ein Chip **14** enthält alle zum Betrieb notwendigen elektronischen Bauteile, vorzugsweise in hoch integrierter Form. Die daran angeschlossene Miniaturspule **15** ist wesentlich kleiner als die Sende- und Empfangsspule **13** des Abstandslesers AL, so daß sie zum Beispiel für den Einbau in eine Uhr geeignet ist. Jeder Nutzer, der Zugang zu dem zu schützenden Datenverarbeitungssystem DV erhalten soll, erhält einen Identifikationsträger ID, durch den der Nutzer eindeutig authentisiert werden kann. Diesen Identifikationsträger ID führt der Nutzer möglichst unverlierbar bei sich. Die Miniaturspule **15** tritt im Fall der Abfrage (**Fig. 1**) mit dem Magnetfeld des Abstandslesers AL in Wechselwirkung. Im Fall der Programmierung (**Fig. 2**) befindet sich die Miniaturspule **15** im Bereich eines ähnlichen Magnetfelds, das von einem Schreibgerät SG erzeugt wird. In diesem Feld kann der Identifikationsträger ID kontaktlos programmiert werden. Mit dem Schreibgerät SG lassen sich beispielsweise 2^{31} verschiedene Identifikationsträger ID programmieren oder sperren. Änderungen der auf dem Identifikationsträger ID gespeicherten Parameter sind jederzeit möglich. Das Schreibgerät SG kann als eigenständige Datenendeinrichtung des Datenverarbeitungssystems DV konzipiert sein; dann steht es beispielsweise an der Pforte eines Betriebsgebäudes. Das Schreibgerät SG kann aber auch mit dem Abstandsleser AL kombiniert sein; dann ist der Identifikationsträger ID über die Datenschnittstelle zwischen dem Abstandsleser AL und dem Personal-Computer DE programmierbar.

Die Identifikationsträger ID werden mit einem numerischen Code programmiert. Diesen Daten werden Sicherheitsinformationen beigemischt. Die Erzeugung erfolgt nach einer geheimen Formel. Der im Speicher des Identifikationsträgers ID abgelegte Datensatz kann nur einmal hergestellt werden. Dadurch ist die Möglichkeit ausgeschlossen, daß mehrere Identifikationsträger ID mit gleichem Code existieren. Der Nutzer selbst definiert die frei zugänglichen Datenmengen, während das Schreibgerät SG und der Abstandsleser AL für die Datensicherheit des Programmiervorgangs und des Abfragevorgangs sorgen. Ein bestimmter Bereich des Identifikationsträgers ID bleibt dem Anwender verschlossen; dieser Bereich kann nur einmal bei der Herstellung programmiert werden. Diese Sicherheitsmaßnahmen zusammen mit einem ausgeklügelten Polynom für die Datenübertragung erlauben einen betriebssicheren Einsatz.

Der Chip **14** enthält alle zum Betrieb notwendigen Funktionseinheiten. Hierzu gehören ein Speicher für die nutzerspezifische Kennung, eine Sendeschaltung zur Übertragung der gespeicherten Daten, eine Empfangsschaltung zur Änderung von Teilen der gespeicherten Daten und eine Schaltung für die Energiegewinnung zum Betrieb des Chips **14**. Der Generator für die Spannungsversorgung des Chips **14** gewinnt die Energie aus dem niederfrequenten magnetischen Wechselfeld. Die integrierte Schaltung **14** speichert im Kennungsspeicher eine mehr als 64 bit (Standardpaßwort) lange, eindeutige Kennung des Nutzers. Diese Kennung liegt nicht flüchtig vor und kann durch Aktivieren des Generators für die Spannungsversorgung ausgelesen werden.

Ein Sendeverstärker liest die Kennungsinformation aus dem Speicher, moduliert sie und übermittelt sie an die Miniaturspule **15**. Über dieselbe Schnittstelle läßt sich die gespeicherte Kennung durch Anschließen an das Schreibgerät SG ersetzen. Der Chip **14** und die Miniaturspule **15** sind geschützt in einen Träger eingebaut. Drei mögliche Bauformen des Identifikationsträgers ID sind in **Fig. 3** dargestellt. Alle Identifikationsträger ID sind mit einer fest angebrachten Seriennummer ausgestattet.

In **Fig. 3.1** sind der Chip **14** und die Miniaturspule **15** wasserdicht in flexibles Material eingegossen. **Fig. 3.1** zeigt ungefähr in natürlicher Größe, wie der so entstandene Miniaturträger an einem Armband **16** befestigt werden kann. Ein Kunststoffring **17** umschließt den Identifikationsträger ID und das Armband **16**, das beispielsweise ein Uhrarmband ist. Der Miniaturträger **14**, **15** kann aber auch mit Hilfe eines nichtmagnetischen Clips an dem Armband **16** befestigt werden.

In **Fig. 3.2** ist ein Uhrgehäuse so gestaltet, daß neben dem Uhrwerk **18** zusätzlich der Chip **14** und die Spule **15** in dem Gehäuse Platz finden. Die Spule **15** liegt in diesem Ausführungsbeispiel an der Umfangslinie des Zifferblattes.

Eine weitere Möglichkeit zur Befestigung des Identifikationsträgers ID in Handnähe ist in **Fig. 3.3** dargestellt. Der Chip **14** und die Miniaturspule **15** sind in ein eigens dafür angefertigtes, nichtmagnetisches Armband **20** eingebettet. Dieses Armband verfügt über einen Verschluß **19**, so daß es außerhalb des Betriebs abgelegt werden kann. Zur weiteren Erhöhung der Sicherheit kann dieser Verschluß mit einem elektronischen Schaltmechanismus kombiniert werden, der die im Chip **14** gespeicherten Informationen löscht, so daß das Armband **20** bei Verlust für den Finder wertlos wird.

Es ist auch denkbar, den Identifikationsträger ID als Fingerring zu realisieren.

In **Fig. 4** ist ein Blockschaltbild des Abstandslesers AL dargestellt, der an jede Datenendeinrichtung DE des zu schützenden Systems DV angeschlossen wird. Bei Bedarf kann der Einsatz des Abstandslesers AL auf solche Datenendeinrichtungen DE beschränkt werden, die nicht durch sonstige Maßnahmen hinreichend geschützt sind oder bei denen ein häufiger Wechsel des Nutzers vorkommt.

Der Abstandsleser AL setzt sich im wesentlichen aus der elektronischen Baugruppe **2** und der Sende- und Empfangsspule **13** zusammen. Die Sende- und Empfangsspule **13**, die aus Kupferdraht besteht, ist über eine zweiadrige Verbindungsleitung **12** mit der elektronischen Baugruppe **2** verbunden. Die elektronische Baugruppe **2** ihrerseits setzt sich in der Hauptsache aus einer Sende- und Empfangsschaltung **8** und einem Mikroprozessor **3** zusammen. Die Sende- und Empfangsschaltung **8** enthält einen Generator **9** mit Leistungsverstärker **10**, der das niederfrequente magnetische Wechselfeld in der Sende- und Empfangsspule **13** erzeugt. Das vom Identifikationsträger ID in die Sende- und Empfangsspule **13** eingekoppelte Signal wird über eine Empfangsschaltung **11** so weit aufbereitet, daß es vom Mikroprozessor **3** ausgewertet werden kann.

Der Mikroprozessor **3** besteht im wesentlichen aus einer CPU **5**, einem EEPROM **6** zur Speicherung des Abfrageprogramms, einem RAM **7** als Arbeitsspeicher sowie aus einem Schnittstellenbaustein **4**. Der Schnittstellenbaustein **4** betreibt, zusammen mit dem Abfrageprogramm, die Schnittstelle **1**. Über diese Schnittstelle **1** wird der Abstandsleser AL an den Personal-Computer oder an eine sonstige Datenendeinrichtung DE angekoppelt. Bei einer bereits realisierten Version ist die Schnittstelle **1** als V.24-Schnittstelle zu einem Personal-Computer realisiert. Bei der in **Fig. 1** dargestellten Ver-

sion, bei der die elektronische Baugruppe 2 des Abstandslesers AL als Steckkarte in die Datenendeinrichtung DE eingesetzt wird, wird die Schnittstelle 1 als interne Bus-Schnittstelle ausgeführt.

Im Betrieb wird über die Leistungskette 9, 10, 12, 13 ein Wechselmagnetfeld begrenzter Reichweite erzeugt, das in der Miniaturspule 15 des Identifikationsträgers ID eine Wechselspannung erzeugt. Diese Wechselspannung wird im Chip 14 in die erforderliche Betriebsspannung umgesetzt. Der Identifikationsträger ID sendet daraufhin die in ihm gespeicherte Nutzerkennung in binärer Form aus. Die Daten werden vom Empfangszweig 13, 12, 11 des Abstandslesers AL empfangen und im Mikroprozessor 3 aufbereitet und ausgewertet. Der Mikroprozessor 3 steuert über die Schnittstelle 1 die Datenendeinrichtung DE an und löst dort frei programmierbare Folgeaktionen aus, die im Zusammenhang mit dem Funktionsflußdiagramm gemäß **Fig.** 6 besprochen werden.

Fig. 5 zeigt eine zu **Fig.** 1 alternative Ausführungsform des Abstandslesers AL. Es handelt sich um ein keilförmiges Gehäuse 23, in dem sowohl die Sende- und Empfangsspule 13 als auch die elektronische Baugruppe 2 untergebracht sind. Das Gehäuse 23 besteht aus mitteldichter Faserplatte (MDF) und wird als Vorlegekeil vor die Tastatur TA eines tragbaren Personal-Computers gelegt. Eine grüne Leuchtdiode 21 auf der Oberseite des Gehäuses 23 zeigt die Anwesenheit eines Identifikationsträgers ID im Wirkungsbereich der Sende- und Empfangsspule 13 an. Der Anschluß an den Personal-Computer erfolgt mit Hilfe eines aus dem Gehäuse 23 herausgeführten Verbindungskabels 22. Das Verbindungskabel 22 wird mit einer der seriellen Schnittstellen des Personal-Computers verbunden.

Das Flußdiagramm in **Fig.** 6 zeigt die wichtigsten Funktionen des im Abstandsleser AL enthaltenen Abfrageprogramms. Im Zustand a "kein Nutzer" ist keine Person mit dem Datenverarbeitungssystem DV in Verbindung getreten. Die Dateneinrichtung DE ist für alle Eingaben gesperrt und keine ihrer Anwendungen ist aktiv. In der Funktion b überprüft die CPU 5 fortlaufend das Signal des Empfängers 11 daraufhin, ob ein Identifikationsträger ID in den Wirkungsbereich der Sende- und Empfangsspule 13 eintritt. Falls ein Identifikationsträger ID detektiert wird, wird die Funktion c aktiv. Mit Hilfe einer Datenbasis, die entweder im EEPROM 6 oder auf den Speichermedien des Personal-Computers DE oder im zentralen Speicher des Datenverarbeitungssystems DV abgelegt ist, wird geprüft, ob die Kennung dieses Nutzers für diese Datenendeinrichtung DE zugelassen ist. Falls nicht, bleibt das Gerät DE gesperrt und es wird gewartet, bis eine neue Kennung detektiert wird.

Falls die Kennung zugelassen ist, wird im Zustand d die Datenendeinrichtung zur Nutzung freigegeben. Die Anwesenheit des Identifikationsträgers ID im Wirkungsbereich der Sende- und Empfangsspule 13 wird durch die Funktion e fortlaufend überwacht. Sobald der Nutzer den Wirkungsbereich verläßt, wird die Datenendeinrichtung DE in näher zu bestimmender Weise gesperrt und auf die Detektion einer weiteren Nutzerkennung gewartet. Der Wirkungsbereich eines Gehäuses 23 oder einer entsprechenden Schreibtischunterlage oder einer sonstigen Bauform der Sende- und Empfangsspule 13 beträgt typischerweise weniger als 20 cm, überschreitet aber aus Sicherheitsgründen in keinem Fall die Entfernung von einem Meter.

Unter dem Blockieren der Datenendeinrichtung welches sofort ausgelöst wird, ist insbesondere ein Sperren der Tastatur und/oder ein Dunkeltasten des Bildschirms zu verstehen. Diese Sperren werden wieder aufgehoben, wenn der Nutzer in den Wirkungsbereich zurückkehrt. Nach Ablauf einer bestimmten Zeit (z. B. drei Minuten) kann das Abfrageprogramm den Nutzer beim Datenverarbeitungssystem DV abmelden (LOGOFF). Bei besonders sicherheitsempfindlichen Datenendeinrichtungen kann auch registriert werden, wenn sich der Nutzer kurzzeitig von der Datenendeinrichtung DE entfernt und diese gesperrt wird. Die Funktion "Sperren der Tastatur/Dunkeltasten des Bildschirms" kann auch ausgelöst werden, wenn ein nicht autorisierter Nutzer in den Wirkungsbereich des Abstandslesers AL kommt. Hierzu sind ggf. weitere Sensoren einzusetzen.

Neben dem automatischen Sperren der Datenendeinrichtungen gibt es für den Nutzer natürlich die Möglichkeit, eine Sitzung explizit zu beenden. Die Funktion f entscheidet darüber, ob alle aktiven Anwendungen beendet werden oder ob die automatischen Sperrfunktionen auslösbar bleiben. Weitere Sperrfunktionen oder Folgeaktionen sind programmierbar, beispielsweise über die Schnittstelle 1 von der Datenendeinrichtung her.

Patentansprüche

1. System zur Authentisierung des Nutzers einer Datenendeinrichtung eines Datenverarbeitungssystems,
bei dem der Nutzer einen Identifikationsträger, der innerhalb einer vorbestimmten Entfernung berührungslos abgefragt werden kann, schwer verlierbar mit sich trägt,
und bei dem ein Abstandsleser, der nahe bei der Datenendeinrichtung angebracht und über ein Verbindungskabel mit der Datenendeinrichtung verbunden ist, eine persönliche Nutzerkennung auf dem Identifikationsträger sich innerhalb der vorbestimmten Entfernung befindet,
dadurch gekennzeichnet, daß
ein Schreibgerät (SG) zu vorgegebenen Zeitpunkten (z. Bsp. täglich) eine neue persönliche Nutzerkennung auf dem Identifikationsträger (ID) einprogrammiert und gleichartig an das Datenverarbeitungssystem (DV) übermittelt,
der schwer verlierbare Identifikationsträger (ID) in der Nähe des Handgelenks des Nutzers angebracht ist,
die vorbestimmte Entfernung zwischen Identifikationsträger (ID) und Abstandsleser (AL) und damit auch die Entfernung zwischen Identifikationsträger (ID) und Datenendeinrichtung (DE) weniger als 1 Meter beträgt
und sowohl die Abfrage als auch die Programmierung der persönlichen Nutzerkennung durch ein magnetisches Wechselfeld vermittelt wird.

2. Authentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß die genutzte Datenendeinrichtung ein Personal-Computer ist.

3. Authentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß die genutzte Datenendeinrichtung eine Workstation ist.

4. Authentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß die genutzte Datenendeinrichtung ein Terminal ist.

5. Authentisierungssystem nach Anspruch 1 bis 4, dadurch gekennzeichnet, daß das Schreibgerät

(SG) die erzeugte Nutzerkennung an die zentrale Datenbasis des Datenverarbeitungssystems (DV) übermittelt.

6. Authentisierungssystem nach Anspruch 1 bis 4, dadurch gekennzeichnet, daß das Schreibgerät (SG) mit dem Abstandsleser (AL) kombiniert ist und die erzeugte Nutzerkennung an die Datenbasis im Abstandsleser (AL) übermittelt.

8. Authentisierungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die vorbestimmte Entfernung zwischen dem Identifikationsträger (ID) einerseits und dem Abstandsleser (AL) bzw. der Datenendeinrichtung (DE) andererseits weniger als 20 cm beträgt.

9. Authentisierungssystem nach Anspruch 1 bis 8, dadurch gekennzeichnet, daß die Datenendeinrichtung (DE) sofort gesperrt wird, wenn der Identifikationsträger (ID) die vorbestimmte Wirkungsentfernung verläßt.

10. Authentisierungssystem nach Anspruch 9, dadurch gekennzeichnet, daß die Eingabetastatur (TA) blockiert wird.

11. Authentisierungssystem nach Anspruch 9, dadurch gekennzeichnet, daß ein Bildschirm der Datenendeinrichtung (DE) dunkelgetastet oder ein Drucker der Datenendeinrichtung (DE) gesperrt wird.

12. Authentisierungssystem nach Anspruch 9, dadurch gekennzeichnet, daß die Datenendeinrichtung (DE) den Nutzer nach Ablauf einer bestimmten Zeitspanne beim Datenverarbeitungssystem (DV) abmeldet.

13. System zur Authentisierung, mit welchem der Nutzer eines Datenverarbeitungssystems, der sich in der Nähe einer Datenendeinrichtung befindet, berührungslos authentisiert wird, gekennzeichnet durch
einen Identifikationsträger (ID), der aus einem Chip (14) und einer Miniaturspule (15) besteht,
einen Abstandsleser (AL), bei dem eine elektronische Baugruppe (2) über eine Verbindungsleitung (12) an eine Sende- und Empfangsspule angeschlossen ist,
und ein Schreibgerät (SG) zum Programmieren des Identifikationsträgers (ID), welches zentral oder über die Datenendeinrichtung (DE) an das Datenverarbeitungssystem (DV) angeschlossen ist.

14. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) an einem Armband (16) befestigt ist.

15. System nach Anspruch 14, dadurch gekennzeichnet, daß die Befestigung durch einen Kunststoffring (17) geschieht.

16. System nach Anspruch 14, dadurch gekennzeichnet, daß die Befestigung durch einen nichtmagnetischen Clip geschieht.

17. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) in ein Armband (20) eingebaut ist.

18. System nach Anspruch 17, dadurch gekennzeichnet, daß das Armband (20) einen Verschluß (19) aufweist, bei dessen Öffnen die Kennung im Identifikationsträger (ID) gelöscht wird.

19. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) neben einem Uhrwerk (18) in einem Uhrgehäuse eingebaut ist.

20. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) in einem Fingerring eingebaut ist.

21. System nach Anspruch 13 bis 20, dadurch gekennzeichnet, daß der Abstandsleser (AL) in einem Gehäuse (23) untergebracht ist, das eine elektronische Baugruppe (2) und eine Sende- und Empfangsspule (13) enthält und als Vorlegekeil ausgebildet ist.

22. System nach Anspruch 21, dadurch gekennzeichnet, daß das Gehäuse (23) eine Leuchtdiode (21) trägt, welche die vollzogene Authentisierung des Nutzers anzeigt.

23. System nach Anspruch 13 bis 20, dadurch gekennzeichnet, daß die Sende- und Empfangsspule (13) des Abstandslesers (AL) in eine Schreibtischunterlage eingewirkt ist, und daß die elektronische Baugruppe (2) des Abstandslesers (AL) auf einer Steckkarte angeordnet ist, welche in die Datenendeinrichtung (DE) einsteckbar ist.

24. System nach Anspruch 13 bis 23, dadurch gekennzeichnet, daß ein Zusatzsensor (ZS) vorgesehen ist, der für die Annäherung des Identifikationsträgers (ID) an eine weitere Eingabevorrichtung, insbesondere eine sog. Maus, empfindlich ist.

25. System nach einem der Ansprüche 13 bis 24, dadurch gekennzeichnet, daß weitere Sensoren vorgesehen sind, welche die Annäherung von nichtberechtigten Personen registrieren.

26. System nach Anspruch 13 bis 25, dadurch gekennzeichnet, daß die elektronische Baugruppe (2) des Abstandslesers (AL) über eine serielle Schnittstelle an die Datenendeinrichtung (DE) angeschlossen ist.

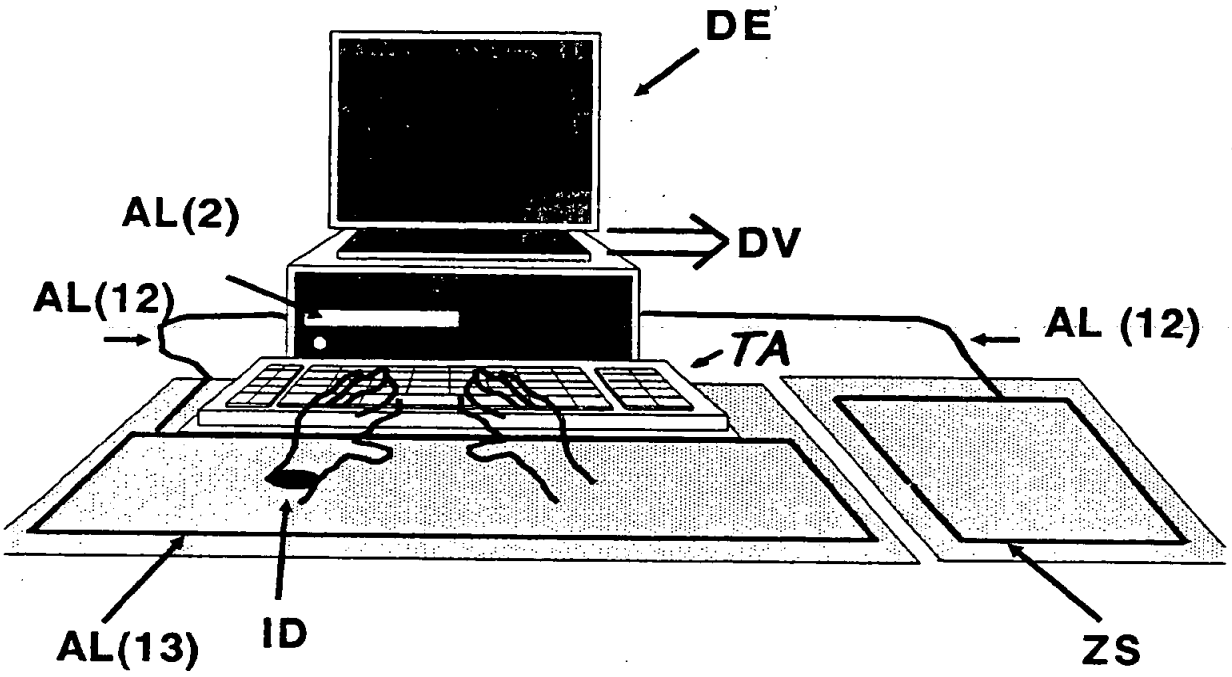
27. System nach Anspruch 13 bis 25, dadurch gekennzeichnet, daß die elektronische Baugruppe (2) des Abstandslesers (AL) über eine interne Schnittstelle an den Datenbus der Datenendeinrichtung (DE) angeschlossen ist.

Hierzu 5 Seite(n) Zeichnungen

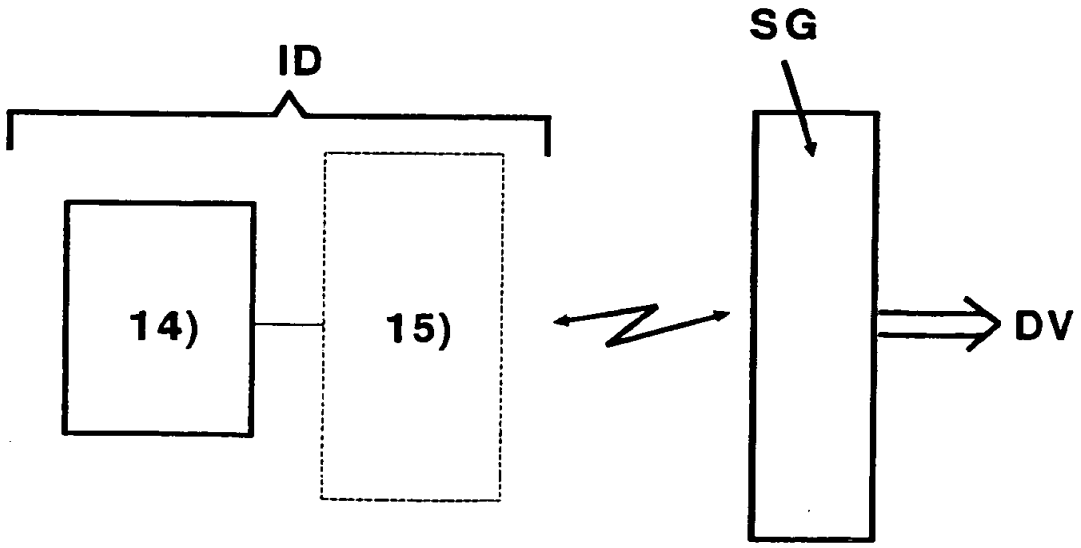
— Leerseite —

Nummer: DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 1: Hauptkomponenten



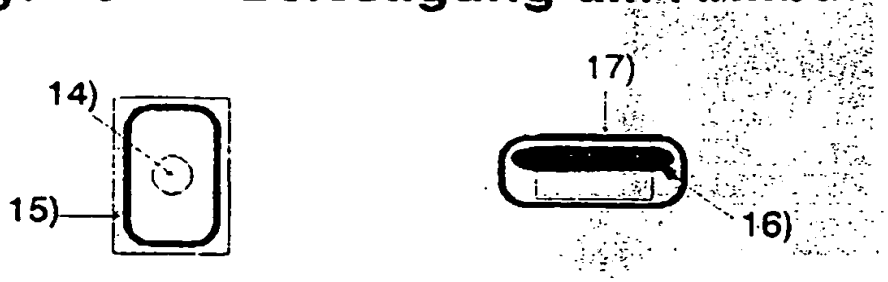
Figur 2: Blockschaltbild des ID-Trägers



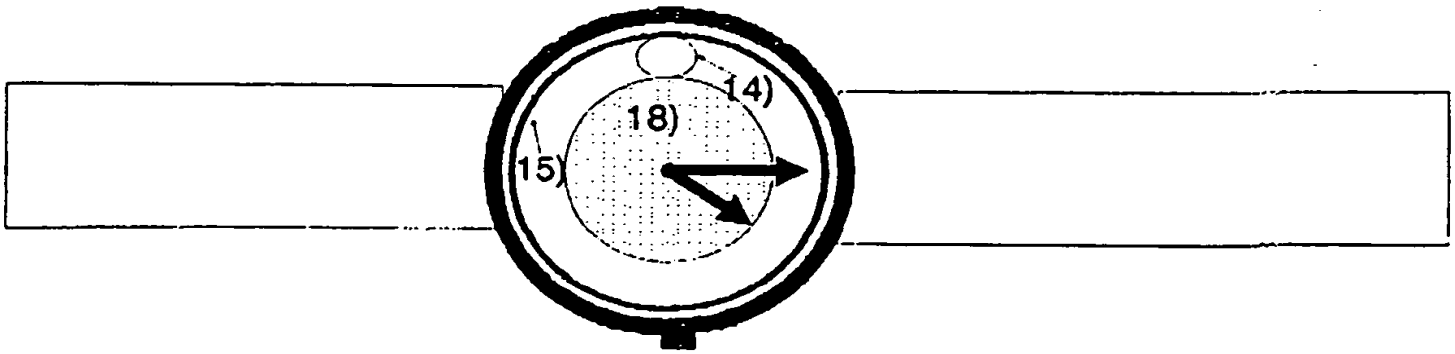
Nummer: DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 3: Bauformen des ID-Trägers

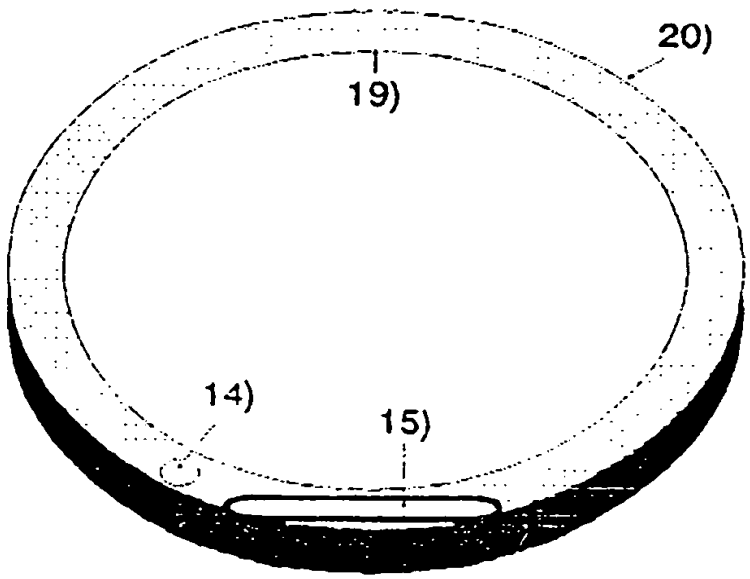
Figur 3.1: Befestigung am Armband



Figur 3.2: in Uhr integriert

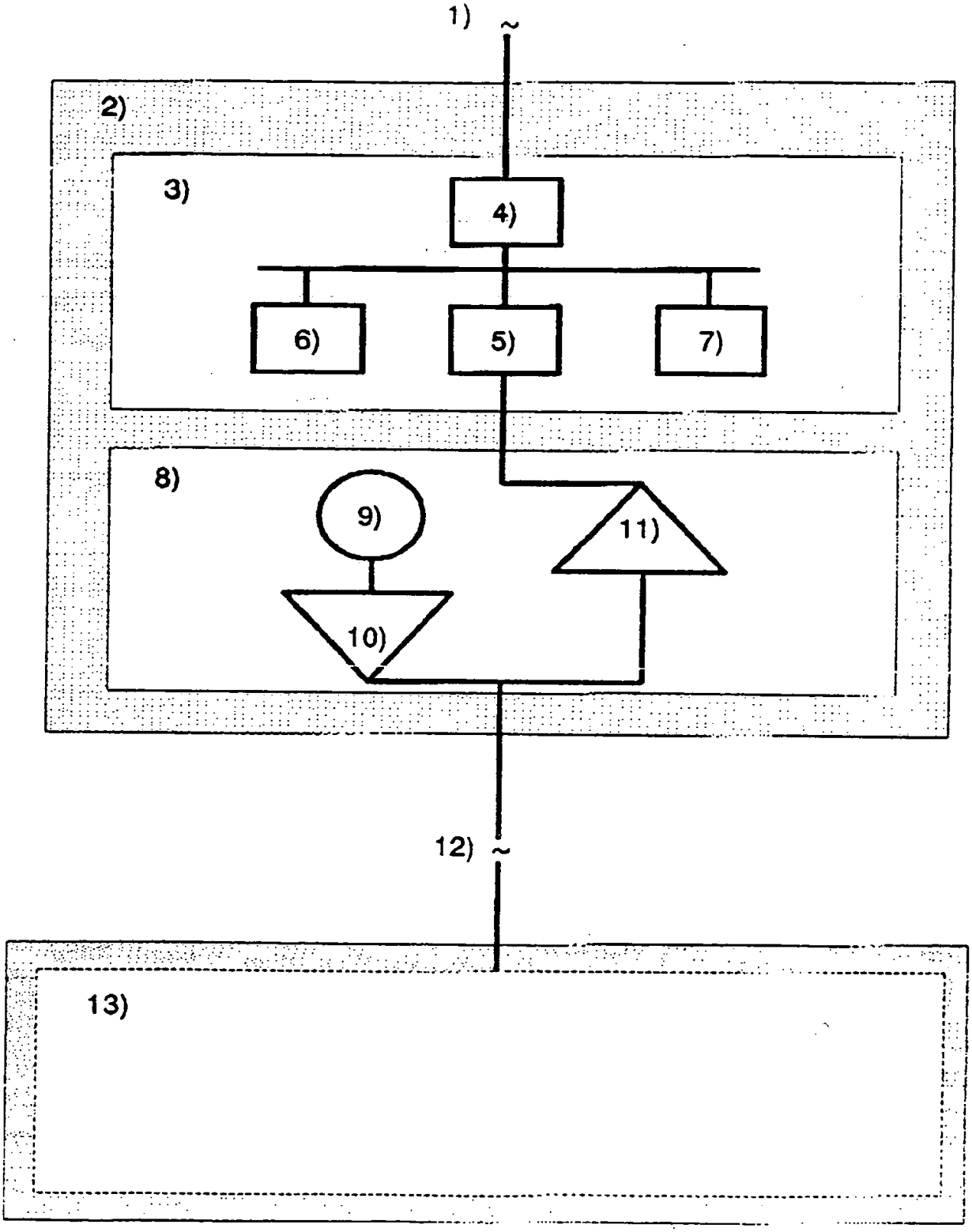


Figur 3.3: in Armband integriert



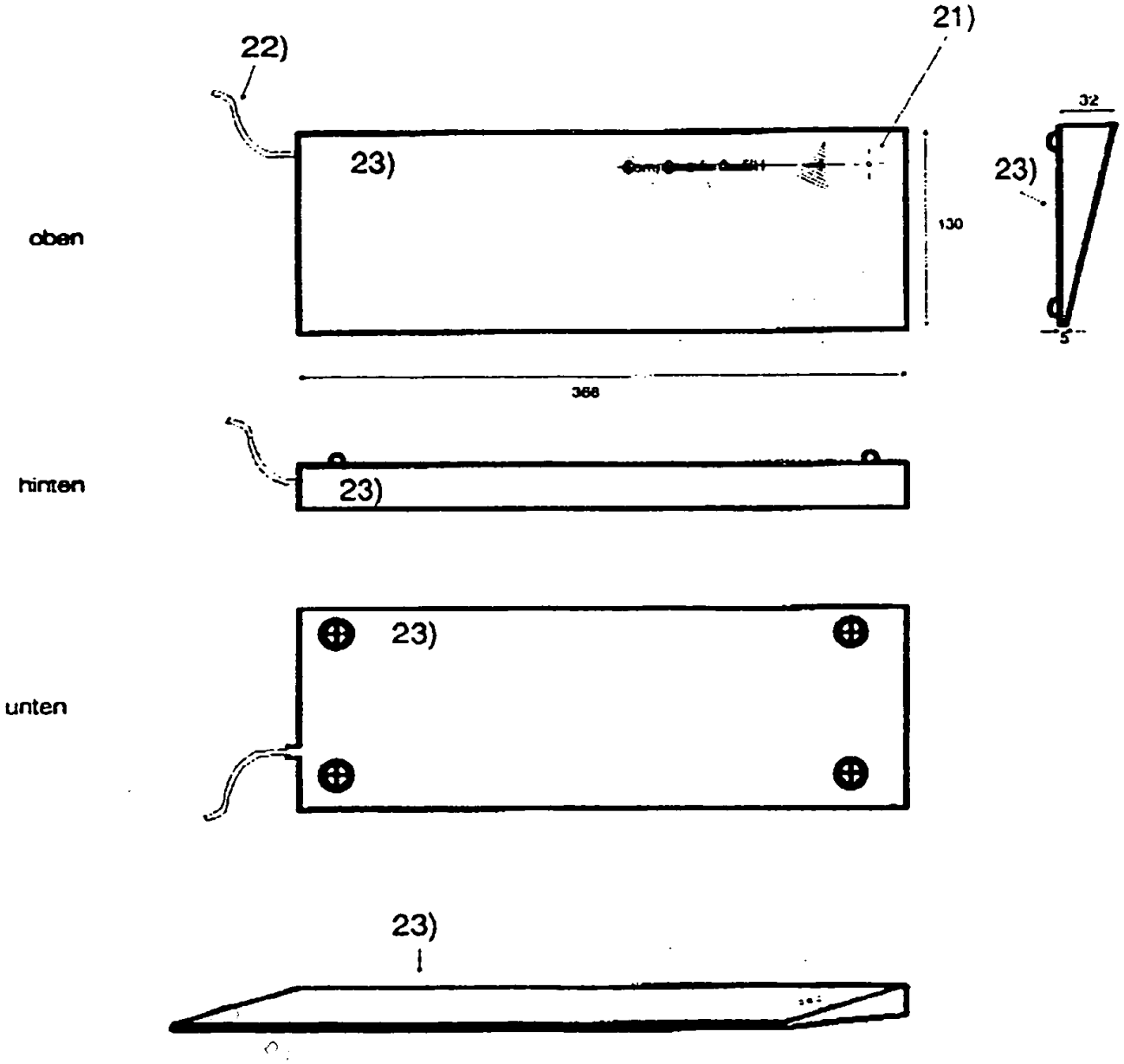
Nummer: DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 4: Blockschaltbild des Abstandslesers



Nummer: DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 5: Gehäuse für Abstandsleser



Nummer: DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 6: Funktionsflußdiagramm